

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED <div style="text-align: center; font-weight: bold;">TOP SECRET</div> b. LEVEL OF SAFEGUARDING REQUIRED <div style="text-align: center; font-weight: bold;">TOP SECRET</div>			
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>				3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>			
a. PRIME CONTRACT NUMBER				a. ORIGINAL <i>(Complete date in all cases)</i>		DATE (YYYYMMDD)	
b. SUBCONTRACT NUMBER				b. REVISED <i>(Supersedes all previous specs)</i>		REVISION NO. DATE (YYYYMMDD)	
X c. SOLICITATION OR OTHER NUMBER <div style="text-align: center;">FA8818-05-R-0005</div>		DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i>		DATE (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.							
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.							
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>							
a. NAME, ADDRESS, AND ZIP CODE TBD				b. CAGE CODE TBD		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> TBD	
7. SUBCONTRACTOR							
a. NAME, ADDRESS, AND ZIP CODE TBD				b. CAGE CODE TBD		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> TBD	
8. ACTUAL PERFORMANCE							
a. LOCATION Space and Missile Systems Center (SMC) Detachment 12 3548 Aberdeen Ave SE Kirtland AFB, NM 87117-5776				b. CAGE CODE N/A		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> 377 SFS/SPAI 4500 Biggs Ave SE Kirtland AFB, NM 87117-5320	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Advisory and Assistance Services (A&AS) Program Manager: John Seward							
10. CONTRACTOR WILL REQUIRE ACCESS TO:				11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:			
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		YES NO		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		YES NO	
b. RESTRICTED DATA		<input checked="" type="checkbox"/> <input type="checkbox"/>		b. RECEIVE CLASSIFIED DOCUMENTS ONLY		<input type="checkbox"/> <input checked="" type="checkbox"/>	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input checked="" type="checkbox"/> <input type="checkbox"/>		c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		<input checked="" type="checkbox"/> <input type="checkbox"/>	
d. FORMERLY RESTRICTED DATA		<input checked="" type="checkbox"/> <input type="checkbox"/>		d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		<input type="checkbox"/> <input checked="" type="checkbox"/>	
e. INTELLIGENCE INFORMATION		<input type="checkbox"/> <input checked="" type="checkbox"/>		e. PERFORM SERVICES ONLY		<input type="checkbox"/> <input checked="" type="checkbox"/>	
(1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/> <input type="checkbox"/>		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		<input type="checkbox"/> <input checked="" type="checkbox"/>	
(2) Non-SCI		<input checked="" type="checkbox"/> <input type="checkbox"/>		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		<input checked="" type="checkbox"/> <input type="checkbox"/>	
f. SPECIAL ACCESS INFORMATION		<input checked="" type="checkbox"/> <input type="checkbox"/>		h. REQUIRE A COMSEC ACCOUNT		<input type="checkbox"/> <input checked="" type="checkbox"/>	
g. NATO INFORMATION		<input type="checkbox"/> <input checked="" type="checkbox"/>		i. HAVE TEMPEST REQUIREMENTS		<input checked="" type="checkbox"/> <input type="checkbox"/>	
h. FOREIGN GOVERNMENT INFORMATION		<input checked="" type="checkbox"/> <input type="checkbox"/>		j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<input checked="" type="checkbox"/> <input type="checkbox"/>	
i. LIMITED DISSEMINATION INFORMATION		<input type="checkbox"/> <input checked="" type="checkbox"/>		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input type="checkbox"/> <input checked="" type="checkbox"/>	
j. FOR OFFICIAL USE ONLY INFORMATION		<input checked="" type="checkbox"/> <input type="checkbox"/>		l. OTHER <i>(Specify)</i>		<input checked="" type="checkbox"/> <input type="checkbox"/>	
k. OTHER <i>(Specify)</i> Program Protection Planning Information		<input checked="" type="checkbox"/> <input type="checkbox"/>		Receive and generate sensitive-but-unclassified (SBU) data; and will have access to the government network			

ANNEX 1
SOLICITATION NO: FA8818-05-R-0005

DD FM 254 GUIDANCE

Remarks pertaining to Sections 10, 11, 12, 13, 14, and 15 are as follows:

1. SECTION 10:

1.1 Contractor personnel must possess a final U.S. Government clearance at the appropriate level and be briefed (as required) for access to the below data. A list of contractor personnel with such accesses will be provided to the SMC Det 12 Security Office upon request. Visit requests must identify access granted and date last briefed as appropriate. The contractor shall apply all applicable markings to the material to include warning notices. All data and materials will be handled, disclosed, transmitted, reproduced and stored in accordance with the NISPOM, Executive Order 12958 as amended and organizational guidance.

1.2 Item 10a. COMSEC Information – See Annex 4 for further guidance

1.3 Item 10e. Intelligence/Sensitive Compartmented Information See Annex 3 for further guidance

1.4 Item 10f. Special Access Information - see Annex 2 for further instructions

1.5 Item 10h. Foreign Government Information. RELEASE OF CLASSIFIED AND UNCLASSIFIED INFORMATION TO FOREIGN GOVERNMENT AND THEIR REPRESENTATIVES: Any military activity or defense contractor receiving a request from a foreign government, or a representative thereof, for classified and/or unclassified information regarding this program shall forward the request through SMC Det 12/RSLP to the Foreign Disclosure Office (FDO), SMC Det 12/MSI for approval. This does not apply to exchange or information on approved foreign military sales programs.

1.6 Item 10j: See DOD 5400.7/AF Sup 1, Chap 4, and, AFI 33-129 for guidance on FOR OFFICIAL USE ONLY information to include transmittal across the internet.

2. SECTION 11:

2.1 Item 11c:

2.1.1 Prospective offeors must have the appropriate facility clearance and a minimum of 10 personnel shall have a current (five years old or less) TOP SECRET clearance at contract start. Other contractor personnel must have or be able to obtain a SECRET clearance within 180 days of contract start. Additionally, in order to gain access to government information systems or contractor-owned systems used to process government data or information ALL contractor personnel must have a national agency check.

2.1.2 The contractor will require access to TOP SECRET information. Any extracts or use of such data will require the contractor to apply derivative classifications and markings consistent with the source from which the extracts were made in accordance with E.O. 12958 as amended.

2.1.1 See under Contract Clauses of the contract, Notification of Government Security Activity Clause, Part II. Work, to include classified automatic data processing, will be accomplished at the prime contractor facilities and Kirtland AFB, NM. When processing classified information on government furnished automated information systems (AIS) the contractor shall comply with all applicable DOD, Air Force, Major Commands and local Security and Protection Guidelines. It is the contractor's responsibility to understand these publications (e.g., directives, instructions, manuals, plans) and to obtain a copy from the office providing support to; the Government Contracting Officer, Security Office, or the Information Assurance Office.

2.2 **Item 11i.** The contractor shall, in addition to the requirements set forth in the DOD National Industrial Security Operating Manual (NISPOM), DOD 5220.22-R, the Use of Commercial Wireless Devices, Services and Technologies in the DOD Global Grid (GIG), DODD 8100.2, Information Assurance, DODD 8500.1, comply with HQ Air Force, HQ AFSPC, applicable host installation , and, local commander written instructions regarding EMSEC. This will include Time Critical Network Orders. Notices to Airmen and other real-time EMSEC-related system and network update requirements.

2.3 **Item 11j:** Operations Security (OPSEC) is an unclassified program design to deny our adversaries access to critical information. OPSEC implementation is an inherent responsibility for all personnel that handles For Official Use Only information and other categories of sensitive information. The government has the responsibility to integrate OPSEC into plans, directives and to develop policy, provide guidance and training. OPSEC education shall be provided to all personnel as part of in-processing and on an annual basis. General environmental awareness and proper safeguarding is the vital link to protect our critical assets. Contractors shall be required to comply with the Det 12 OPSEC Instruction in performance of day-to-day duties.

2.4 **Item 11l:** Sensitive-but-Unclassified (SBU) automatic data processing will occur at the prime contractor facilities and Kirtland AFB, NM. The contractor will also be granted access to networks at these locations or interface between these sites via the Internet. When processing SBU information on either government-furnished or contractor systems, ADPE prior approval must be granted by the SMC Det 12 Information Assurance Office. Information of an SBU nature will not be placed on the Internet without approved and tested access and security controls. This includes information that falls under the definition of Personal or Privacy Act, FOR OFFICIAL USE Only, Scientific, Technical or Research and Development.

3. SECTION 12:

There will be no voluntary public release of information. Requests for public release of information concerning this contract shall be submitted through SMC Det 12/RSLP to SMC Det 12/CCX as appropriate, 45 days in advance of scheduled release date. Answers to queries may be made only with the express approval of the SMC Det 12/CCX, 3548 Aberdeen Ave SE, Kirtland AFB NM 86117-5606. No other dissemination of information is authorized. This prohibition extends to all publications of an informational nature both internal and external, and to all conversations except those required for conduct of official business.

4. SECTION 13:

4.1 Classified information may be transmitted through the Internet if encrypted utilizing National Security Agency approved encryption methods. Only FDO approved releasable public information may be directly accessed from the Internet without access controls. All information maintained on a computer system connected to the Internet and not protected by access controls must be public access information. The following types of unclassified information **shall not** be placed on the Internet without approved and tested access and security controls: (a) For Official Use Only; (b) Personal or Privacy Act; (c) Scientific, Technical or Research and Development; and, (d) Unclassified information that requires special handling. Refer to DOD 5400.7/AF Sup 1, Chap 4 to address FOR OFFICIAL USE ONLY application.

4.2 Refer to Annex 5, Other Security and Protection Measures, with regard to Security Classification Guidance and Program Protection Information.

5. SECTION 14: Additional security requirements, in addition to the NISPOM and associated annex(es), are established. Contractor personnel providing direct support to SMC and permanently assigned to Kirtland AFB will abide by the provisions set forth in the Visitor Group Security Agreement and cooperate under the local security authority oversight. Refer to the appropriate annex to the DD Fm 254 for these requirements and guidelines.

6. SECTION 15: Defense Security Service is the inspection authority for all collateral classified work efforts. SMC/INS, Los Angeles AFB, CA is the authority for all SCI related matters

ANNEX 2
SOLICITATION NO: FA8818-05-R-0005
SPECIAL ACCESS INFORMATION

Special Access Information:

- a. The contractor shall establish a point of contact for Special Access Required (SAR) security matters. This individual will have responsibility for all SAR security matters within the contractor's facility, in accordance with the appropriate SAR Security Guide.
- b. The contractor shall establish and maintain an access list of those employees approved by the contract monitor for SAR portions of the contract. A copy of this list will be furnished to SMC Det 12 Security Office.
- c. The Contractor will comply with all Program Protection Plans/System Protection Guides specified in the applicable Delivery Order Statement of Work or the contract DD Form 254.
- d. The Contractor will require access to classified information/material up to and including TOP SECRET and TOP SECRET/SAR. All elements of this contract for SAR information or material are under the cognizance of SAF/AAZ.
- e. The contractor will advise SMC Det 12 Security Office immediately upon reassignment of briefed personnel to other duties not associated with this contract.

ANNEX 3
SOLICITATION NO: FA8818-05-R-0005

SENSITIVE COMPARTMENTED INFORMATION

1. GENERAL

a. Physical Security

This contract requires access to Sensitive Compartmented Information (SCI). The Director of Intelligence, Surveillance, and Reconnaissance / Deputy Chief of Staff, Air and Space Operations, USAF, has exclusive security responsibility for all SCI classified material released to or developed under this contract. This SCI information must be maintained in a Sensitive Compartmented Information Facility (SCIF). DCID 6/4, 6/9, DoD 5105.21-M-1 and AFMAN 14-304 serve as the necessary guidance for physical, personnel, and information security measures and are part of the security specification for this contract. Contractor compliance with these directives is mandatory unless specifically waived. Inquiries pertaining to classification guidance for SCI will be directed to SMC/INS through the Contract Monitor. The contractor is required to comply with the physical security standards as defined in DCID 6/9, DOD 5105.21-M-1 and AFMAN 14-304. SCI material released to the contractor under this contract shall be stored and worked on only within the proposed facility and upon receipt of an approved physical security accreditation by SSO DIA/DAC. AFSPC sponsored SCIF shall not be co-utilized with other government agencies unless covered by an approved Co-Utilization Agreement (CUA). The User Agency SSO is SMC/INS, Los Angeles AFB, CA. Work performed under this contract shall not be accomplished in a SCIF accredited by another Government Organization unless there is an approved CUA between that organization and SMC/INS. Applicable Program Security Classification guidance will be identified in block 13 of this DD Form 254.

b. Personnel Security

The contractor shall nominate a CSSO and Alternate to SMC/INS. No contractor will be granted access to SCI information/material under this contract unless they are filling a SMC/IN SCI billet assigned under this contract. The names of contractor personnel requiring accessing to SCI will be submitted to SMC/INS through the Contract Monitor. Upon receipt of a completed background investigation the CSSO will submit a request for SCI eligibility to SMC/INS in accordance with AFMAN 14-304. Contract employees sponsored by other Agencies/Organization shall be certified to SMC/INS through the Servicing SSO for access to SMC Programs. The contractor shall establish and maintain a current billet roster indicating admittance of SCI personnel on this contract. A copy of this list shall be provided to SMC/INS through the Contract Monitor annually, or as changes occur. The contractor shall also advise SMC/INS through the Contract Monitor

immediately upon the reassignment of personnel to duties not associated with this contract, to include termination.

c. Document Control

SCI furnished in support of this contract remains the property of the SMC Program Office releasing it. The contractor shall maintain an active accountability of all SCI material received, produced, maintained, and disposed of that is in their custody. Upon completion or cancellation of this contract, SCI data will be returned to the custody of the SMC Det 12 unless a follow-on contract specifies that material will be transferred to that contract. Inventories of SCI material will be conducted in accordance with DOD 5105.21-M-1 and AFMAN 14-304. Any supplemental instructions will be furnished and/or made available to the contractor through the Contract Monitor by the User Agency Special Security Office (SMC/INS)

d. Release of Information

SCI will be released to contractors only when originator approval has been obtained. The contractor may release such material to any contractor employee assigned to a billet and indoctrinated for Program SCI access under this contract and only when a need-to-know exists. The contractor may release such material to any Special Security Office personnel assigned to HQ SMC, HQ Air Force Space Command (AFSPC), HQ USAF, or DIA upon demand. The contractor shall not release this material to other contractors, subcontractors, or Federal Government agency employees unless the Program Office, Contract Monitor, or SMC/INS has granted prior written approval. An access certification to an SMC contractor occupied SCIF does not constitute approval to release SMC contractual material to other contractors, subcontractors, or federal government employees: SMC/INS or Contract Monitor approval is required. SCI will not be released to non-U.S. citizens. SMC/INS approval of an SMC contractor visit certification or permanent certification to another facility will constitute approval to discuss contractual information/material at the facility to be visited.

e. Reproduction of SCI Information

The contractor may reproduce any SCI related to this contract at the discretion of the Contract Special Security Officer (CSSO), as long as the copies are controlled in the same way as the originals and they remain in the SCIF. No copies of SCI documents will be transferred to other contractors.

f. Sub-Contracting

A CSSO shall coordinate with the Contract Monitor and obtain the concurrence of SMC/INS prior to subcontracting any portion of SCI efforts involved in this contract.

g. Public Release

The contractor shall not make references to SCI even by unclassified acronyms, in advertising, promotional efforts, or recruitment for employees.

h. Block 10k: Other: Automated Information Systems

Comply with DOD 5105.21-M1 Chapters 7 and 8, DIAM 50-4, AFMAN 14-304 Chapters 7 & 8. The Contractor CSSO shall submit a Systems Security Concept of Operations and an AIS Security Operations Procedure/Standard Practice Procedure.

i. Block 11i: TEMPEST Requirements

TEMPEST security measures must be considered if electronic processing of SCI is involved in accordance with DOD 5105.21-M1 Chapter 7 and Appendix J; AFM 14-304, Chapter 7

j. Block 11k: Defense Courier Service

This contract requires the use of the Defense Courier Service (DCS). The CSSO will prepare and submit DCS Form 10 in original triplicate to SSO SMC/INS for validation prior to their submittal to the appropriate DCS station (reference to Block 11k).

k. Block 14: Additional Security Requirements

The following Directives, Manuals, Instructions, Handbooks, or Pamphlets are incorporated into this contract as they pertain to the access, handling, control, dissemination, processing of Sensitive Compartmented Information:

DCID 6/4
DCID 6/9
DOD 5105.21-M1
DIAM 50-4
AFMAN 14-304

l. Block 15: Inspections

Defense Security Service is relived of inspection responsibilities pertaining to Sensitive Compartmented Information associated with this contract. The following activity is designated as inspection authority and the User Agency SSO for SCI requirements in accordance with DOD 5105.21-M-1, and AFMAN 14-304.

SMC/INS (SMC SSO)
2420 Vela Way, Suite 1866
Los Angeles AFB

15 September 2005

El Segundo, CA 90245-4659

The User Agency Special Security Officer (SSO) is:

SMC/INS
(310) 363-1585

The Alternate Special Security Officer (ASSO) is:

SMC/INS
(310) 363-2263 or 1989

- m. The contractor will handle all SCI and non-SCI intelligence information in accordance with the markings and restrictive caveats. All security classification guidance will be derived from source documents. Additional security classification guidance, if required, will be obtained from the source of the SCI information.

(2) Non-SCI

Provisions for the handling of Non-SCI or "Collateral" Intelligence by contractors is governed by Chapter 9, Section 3 of DoD 5220.22-M, the National Industrial Security Program Operating Manual, 1995 (NISPOM). Particular emphasis is placed on the contractor(s) correctly understanding and heeding intelligence portion markings.

As classified material, collateral intelligence will be afforded the same protections, safeguards and precautions required by any classified material unless special intelligence related handling instructions are additionally imposed. These basic safeguards are found in DOD 5200.1-R, Information Security Program and AFI 31-401, Information Security Program Management. The disclosure or release of intelligence derived information, whether its status is collateral or SCI is not authorized without the prior consent of SMC/IN.

- a. NISPOM Supplement Overprint with PCSO Implementer
- b. DCID's, 6/4, and 1/21
- c. Joint DODIIS / Cryptologic SCI Information Systems Security Standards, 28 Mar 97 (FOUO)
- d. DoD 5105.21-M-1

ANNEX 4
SOLICITATION NO: FA8818-05-R-0005
COMMUNICATIONS SECURITY (COMSEC) MEASURES

1.0 GENERAL. The contractor shall, in addition to the requirements set forth in the DoD National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22-R), and the COMSEC Annex (DOD 5220.22-S) comply with the written instructions of the installation Commander regarding communications security matters.

2.0 PURPOSE. Provides for additional security measures required by the Government to be taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications. COMSEC protection results from the application of security measures to electrical systems which generate, handle, process, or use national security information.

3.0 REFERENCE. Item 11h of the DD Fm 254

4.0 COMSEC AND/OR CRYPTOGRAPHIC ACCESS

4.1 COMSEC material/information may not be released to DoD contractors without Air Force Cryptological Support Center (AFCSC) approval. Contractor must forward request for COMSEC material/information to the COMSEC Officer through the program office. The contractor is governed by NSAM 90-1, Oct 2001 for the control and protection of COMSEC material/information. Access to COMSEC material/information is restricted to U.S. citizens holding final U.S. government clearances and is not releasable to personnel holding only a reciprocal clearance.

4.2 The Air Force program/project manager shall designate the number of personnel requiring cryptographic access. The number will be limited to the minimum necessary and will be on a strict need-to-know basis.

4.3 The COMSEC/CRYPTO briefing applies only to the use and control of crypto equipment and specialized COMSEC publications. NACSIM/NACSEM documents are not considered COMSEC controlled material. Additionally, cryptographic information/equipment will not be retained in a contractor facility.

5.0 INTERNET POLICY AND ENCRYPTION

5.1 Classified information may be transmitted through the Internet if encrypted utilizing National Security Agency approved encryption methods. Only releasable public information may be directly accessed from the Internet without access and/or security controls. All information maintained on a computer system connected to the Internet and not protected by access controls, must be public access information.

ANNEX 5
SOLICITATION NO: FA8818-05-R-0005

OTHER SECURITY AND PROTECTION MEASURES

1.0 SECURITY CLASSIFICATION GUIDES

Security Classification Guides (SCG) to include any changes or revisions will be provided to the contractor by SMC Det 12/MSS (Security Office).

2.0 PROGRAM PROTECTION PLANS

The National Security Policy and DOD Space Policy and supplements require RDT&E entities to develop protection plans for major systems and support capabilities. Contractor agencies will be required to participate (i.e. provide existing document and attend meetings) in applicable protection plans development. Protection plans to include any changes or revisions will be provided to the contractor by SMC Det 12/MSI (Information Assurance Office).

3.0 PROGRAM PROTECTION PLANNING

The Air Force will integrate security needs and requirements into a PPP beginning in Phase 0 of an acquisition program and maintain this plan throughout the system's life. Contractor agencies will be required to participate (i.e., provide existing documents and attend meetings) in applicable PPP development and provide a Program Protection Implementation Plan (PPIP) for its respective contractor sites as applicable. The PPP to include any changes or revisions will be made available to the contractor in the performance of the contractual tasks as required.

4.0 CLASSIFICATION CHALLENGES

Requests to challenge information classification, or to have information declassified or downgraded outside of its specified time, should be submitted through the SMC Det 12 Security Office for OCA and DDA action. Pending an OCA or DDA reply the classified information will be handled at its current level of classification.

5.0 INTERNATIONAL PROGRAMS SECURITY

Any classified or controlled unclassified military information (CUMI), also known as controlled export technical data, and technology to be released must be approved by the Foreign Disclosure Office (through SMC Det 12/MS to SMC/AXP) prior to release.